UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/944,788 | 08/31/2001 | Alfonso De Jesus Valdes | 10454-022001/P-4190-4 | 1821 |

52197 7590 09/22/2008

PATTERSON & SHERIDAN, LLP
SRI INTERNATIONAL
595 SHREWSBURY AVENUE
SUITE 100
SHREWSBURY, NJ 07702

| EXAMINER | |
|---|---|
| SHERR, CRISTINA O | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 3685 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 09/22/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/944,788 | VALDES ET AL. | |
| | Examiner | Art Unit | |
| | CRISTINA OWEN SHERR | 3685 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *27 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) *3-6,9-12,15-19,22,23,26,27 and 30* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,7,8,13,14,20,21,24,25,28 and 29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *August 25, 2008 (one such statement), February 21, 2008 (twenty such statements)*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This communication is in response to applicants' amendment filed August 27, 2007. Claims 1, 2, 7, 8, 13, 14, 20, 21, 24, 25, 28 and 29 are currently under examination. Claims 1-30 are currently pending in this case. Claims 1, 2, 7, 8, 13, 14, 20, 21, 24, 25, 28, and 29 are currently amended.

### *Information Disclosure Statement*

2. The information disclosure statements (IDS) submitted on August 25, 2008 (one such statement), February 21, 2008 (twenty such statements) are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements are being considered by the examiner.

### *Response to Arguments*

3. Applicant's arguments filed August 27, 2007 have been fully considered but they are not persuasive.

4. Applicant argues, regarding claims 1, 7, 13, 20, 24 and 28, that nothing in the cited reference discloses, teaches or suggests "comparison of an alert (indicating an attack or anomalous incident) - or more specifically, the comparison of features of the alert - to the features of existing alert classes, in order to classify the alert". Examiner respectfully disagrees and directs attention to Nine et al as follows. In Nine, "Upon receipt of the ticket, receiver process 250 parses the ticket and uses the information in the ticket to query accounting engine 248 for information on where to place the pending ticket (step 538)." (col 8 ln 38-41). In parsing the ticket, the receiver is taking features of the alert then comparing them to other alerts and classifying the

alert, which is deciding where to place the pending ticket. In other words, the pending ticket gets placed with similar pending tickets, which are those in the same class. The class is decided by comparing the features of the ticket to features of other tickets.

5. Further, it follows obviously that if the features obtained in parsing the ticket or alert are very different from all other alerts, then the instant alert cannot be placed with others, and will eventually form its own class.

***Claim Rejections - 35 USC § 112***

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1, 2, 7, 8, 13, 14, 20, 21, 24, 25, 28 and 29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. The terms such as, "potentially similar" and "minimum similarity" constitute relative language, and, as such, are unclear. Thus, the claims fail to properly set forth the metes and bounds of the invention.

9.

***Claim Rejections - 35 USC § 103***

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 2, 7, 8, 13, 14, 20, 21, 24, 25, 28 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nine et al (US 6,560,611).

12. Regarding claim 1 –

13. Nine discloses in an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, the method comprising the steps of:

(a) receiving a new alert (called "message" at col 3 ln 25-30);

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes(e.g. col 3 ln 12-20);

(c) updating a minimum similarity requirement for one or more features (e.g. col 5 ln 50-col 6 ln 10);

(d) updating a similarity expectation for one or more features (e.g. col 5 ln 50-col 6 ln 10);

(e) comparing the new alert with one or more alert classes, and either:

(f 1) associating the new alert with the existing alert class that the new alert most closely matches (col 7 ln 22-46); or

(f 2) defining a new alert class that is associated with the new alert (col 9 ln 5-22).

14. Although Nine discloses messages rather than "alerts", the said messages are the functional equivalents of alerts, where generally, the disclosure of Nine may be adapted by one of ordinary skill in the art to obtain the instant application.

15. Regarding claim 2 –

16. Nine discloses the method of claim 1 further comprising the step (a) of passing each existing alert class through a transition model to generate a new prior belief state for

17. each alert class (e.g. col 5 ln 60- col 6 ln 10).

18. As above, although Nine discloses messages rather than "alerts", the said messages are the functional equivalents of alerts, where generally, the disclosure of Nine may be adapted by one of ordinary skill in the art to obtain the instant application.

19. Claims 7, 8, 13, 14, 20, 21, 24, 25, 28 and 29 are rejected under the same criteria as above.

20. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

***Conclusion***

21. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

22. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CRISTINA OWEN SHERR whose telephone number is (571)272-6711. The examiner can normally be reached on 8:30-5:00 Monday through Friday.

24. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin L. Hewitt, II can be reached on (571)272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

25. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Cristina Owen Sherr
Patent Examiner, AU 3685

/Calvin L Hewitt II/

Supervisory Patent Examiner, Art Unit 3685